STATE OF WASHINGTON

Enterprise Active Directory

WA.LCL Welcome Kit

December 12, 2002

Prepared by: Microsoft Consulting Services. This document is updated as needed and is shared among team members and other involved personnel.

DATE	Rev.	DESCRIPTION	AUTHOR	SIGN OFF
11/30/01	1.0	Initial Version	Anthony Witecki, MCS John Sadie, DSHS Scott Rehm, LNI	
3/27/02	2.0	Redirection of document toward executive management	Barbara Popovsky, Anthony Witecki, MCS	
6/27/02	2.1	Added Training Appendix	John Ditto, DIS	
10/25/02	2.2	New Benefits page 7	Keith Kawamura, GA	
12/12/02	2.2	Final Edits	John Ditto, DIS	

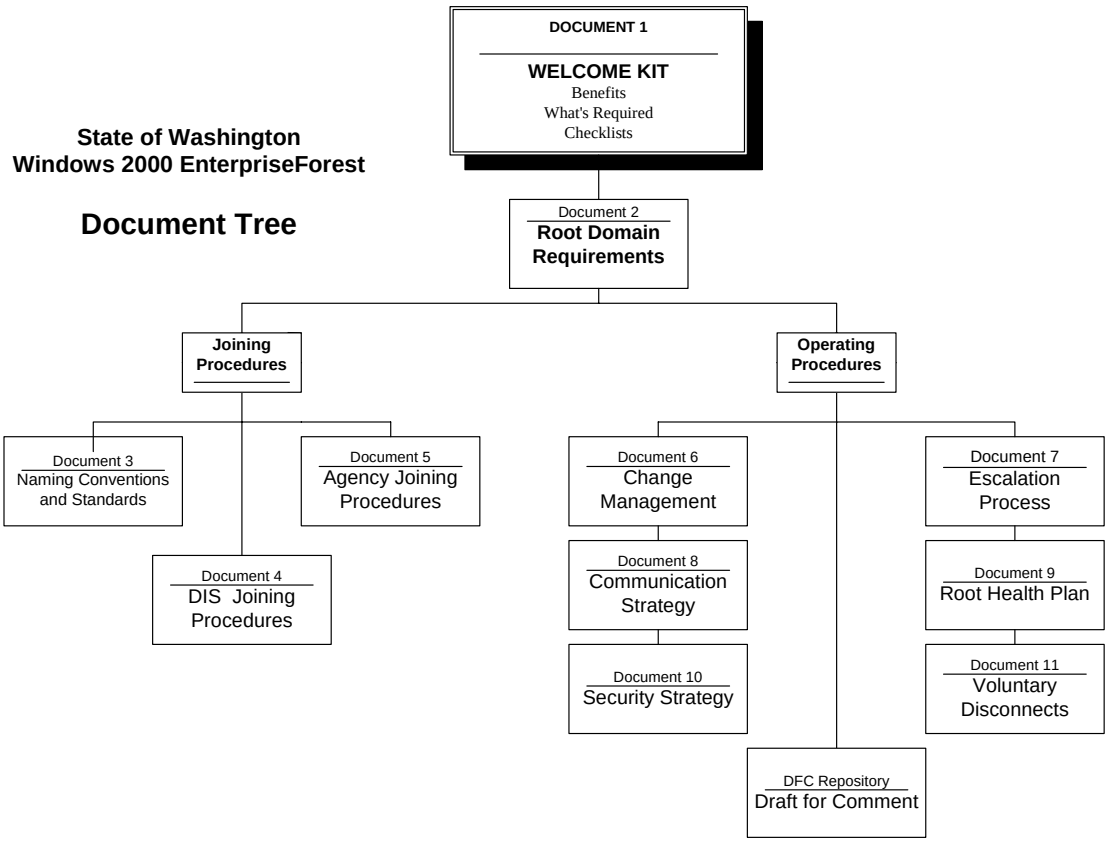
Table of Contents

WELCOME TO THE WINDOWS 2000 ENTERPRISE FOREST

Welcome to the State of Washington Windows 2000 Enterprise Forest !

This visionary Windows 2000 Enterprise Forest is designed to ease data sharing across Washington State agencies and continue to make our State a leader in the Digital Community. This project, spearheaded by the Windows 2000 Forest Architecture Project Steering Committee, is a hallmark of cooperation and forward thinking.

DOCUMENT TREE



To introduce Washington State agencies to their roles and responsibilities in the Windows 2000 Enterprise Forest, a series of documents will guide both management and technologists through the process. The following illustration describes the relationship among the various documents.

Figure 1 - Windows 2000 Enterprise Forest Document Tree

Each document in the series addresses some aspect of implementation of the Windows 2000 Enterprise Forest, beginning with this document–the Welcome Kit–which serves as a general introduction for the forest and is written for a management audience.

The remaining documents in the series describe implementation procedures, which are divided into two categories: joining procedures and operating procedures. Each of the following documents have a management overview and technical content for employees who are responsible for technical implementation of the project. For example, the Root Domain Requirements document is written for technologists and explains the technical requirements for the forest root to be up and running.

Initial agencies participating in the Windows 2000 Enterprise Forest Project include: Department of Social and Health Services (DSHS), Employment Security Department (ESD), Department of Financial Institutions (DFI), General Administration (GA), Labor and Industries (L&I), Office of Financial Management (OFM), Department of Personnel (DOP), Department of Information Services (DIS), Department of Transportation (DOT) and Department of Licensing (DOL).

THE WELCOME KIT

This Welcome Kit provides what you need to know in order to participate in the Windows 2000 Enterprise Forest. Its content includes:

- A brief overview, history and current status of the Forest
- The Vision and Scope for the Forest set by the Steering Committee,
- An explanation of benefits for managers, the agency, the State and the taxpayer,
- Instructions for joining the Enterprise Forest along with agency responsibilities,
- Checklists for joining the Enterprise Forest,
- Supplementary technical detail in accompanying appendices.

WHAT IS THE WINDOWS 2000 ENTERPRISE FOREST ?

The Windows 2000 Enterprise Forest is a collection of one or more Windows 2000 Active Directory Domains . They are organized as peers and connected by trust relationships between an empty Root Domain. All Domains in the Forest share a common schema, configuration, and global catalog.

The Windows 2000 Enterprise Forest has three main purposes:

1. Allow sharing of applications for agencies.
2. Make management easier, by acting as a container for multiple domains.
3. Make the structures transparent to the user.
4. Create a common global catalog (enterprise-wide directory).

Currently, State agencies have separate, multiple, Windows NT domains, Novell Trees and other domains that make information sharing difficult. Working together with the Windows 2000 Steering Committee, agencies can reduce the multiple directories servicing applications, and thus leverage the meta-directory, replication, and security features of Windows 2000. This has the possibility of lowering operating and maintenance costs by reducing the number of domains and domain controllers needed to maintain agency networks.

HISTORY OF THE WINDOWS 2000 ENTERPRISE FOREST

In 1999, following an unsuccessful attempt to organize a single multi-agency Forest, the LAN Managers Group appealed to the Infrastructure Subcommittee of the Customer Advisory Board (CAB) for assistance. In winter 2000, after success of the CAB Pilot, the Board recommended development and implementation of a single Enterprise Forest for the State of Washington. The Windows 2000 Steering Committee was formed with a kickoff meeting in 2000. (Its Vision and Scope are presented later in this section.)

The stated objectives of the Windows 2000 Enterprise Forest are to:

- Create a State of Washington Enterprise Forest with a statewide root for agencies to join,
- Implement the first version of the Active Directory,
- Provide a foundation to allow shared applications and data among agencies,
- Establish statewide governing policies for the Windows 2000 Enterprise Forest,
- Implement Exchange 2000.

What is Active Directory?

Active Directory is a scalable, shared, replicated database of user and other information. It manages authentication and access control for your Windows 2000 environment, and it's an integral part of the Windows 2000 operating system. A partial copy lives on every domain controller.

In joining the States Enterprise Forest, which uses Active Directory, you can take advantage of policy-based network configuration, a built-in user directory, and a platform to share applications.

Delegating administration within the State Forest is another feature that will change the way we need to and will think about IT administration.

STATUS OF THE WINDOWS 2000 ENTERPRISE FOREST

The project has enjoyed a much-anticipated success, celebrating the following accomplishments:

- The Pre-production Forest is up and running,
- Many Agencies have joined the Pre-production Forest, others are ready to join,
- The Production Forest came on line May 2001.
- Standards documentation for the Forest has been developed,
- A governance model for the Forest has been established,
- A web site exists for the project: http://sww.wa.gov/win2k/
- For a list of agencies that have joined the Statewide Forest contact DIS.

To cover the estimated annual costs of $250,000-$300,000, agencies are charged usage based on a proposed cost model that apportions costs by OFM's FTE count for each agency. The Service Level Agreement (SLA) is listed in Appendix B.

GOVERNANCE MODEL

This is the governance model for the Windows 2000 Enterprise Forest. It is currently in practice and working successfully to resolve issues as they emerge.

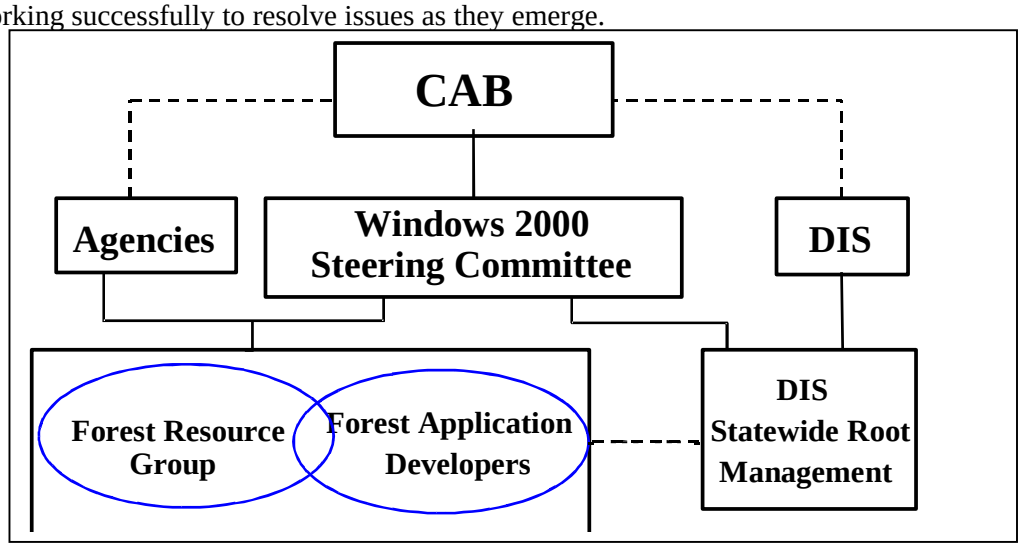


Figure 2 - Windows 2000 Enterprise Forest Governance Model

Relationships among the Governance Components

The Customer Advisory Board (CAB) authorized the Windows 2000 Enterprise Forest in 1999. To oversee the project, the CAB Architecture Subcommittee formed the Windows 2000 Steering Committee from among its members. In turn, the Steering Committee created a project team called the Forest Resource Group (FRG), which consists of representatives supplied by several key agencies, and the Forest Application Developers (FAD). State Agencies and the Department of Information Services (DIS) collaborate with the Steering Committee to develop the Forest.

Roles of the Governance Components

The Windows 2000 Steering Committee was formed by the CAB to spearhead the Enterprise Forest. This committee considers issues of policy and assists the Forest Resource Group (FRG) and Forest Application Developers group (FAD) in matters of business, process and project scope. Many agencies are represented and collaborate in making all of these groups successful.

FRG facilitates the establishment of the Windows 2000 Enterprise Forest, architects the network infrastructure, resolves technical issues, and researches and authors Forest documentation.

The Forest Application Developers group (FAD) defines strategic direction for the Active Directory and makes recommendations to the Steering Committee on the Active Directory schema, application use of the Active Directory, and approval of applications that use the Active Directory. (can you add a link to the current membership?)

The Department of Information Services (DIS) provides project management, contracted technical support from Microsoft, and LAN engineers to design, implement and administer the Windows 2000 Enterprise Forest Root.

WINDOWS 2000 STEERING COMMITTEE VISION

Long Term Vision

The State of Washington Windows forest architecture will be a secure environment in which Active Directory domain objects are available to appropriate personnel of participating state agencies to support the view of one government to citizens, businesses, and other governments.

Short Term Vision

The first release of the State of Washington Windows 2000 single forest will be a coordinated effort by state agencies. It will be a secure environment in which Active Directory domain objects allow each participating state agency to operate independently of other state agencies while improving systems administration, reliability, and security. It will preserve the existing Exchange organization and prepare the foundation for Exchange 2000.

The next key release would enable Exchange 2000 implementations and enable agencies to share objects securely.

Vision and Scope for the Windows 2000 Enterprise Forest
Windows 2000 Steering Committee, March, 9 2001

WINDOWS 2000 STEERING COMMITTEE SCOPE

Long Term Scope

The State of Washington Windows forest architecture will be available for state agencies to join, based on meeting well established and published criteria for participation.

The State of Washington Windows forest will support networking operations, file and print, messaging and collaboration including Exchange, and applications.

Short Term Scope

The initial scope of the State of Washington Windows 2000 single forest will focus on the networking operating system for security, reliability, and improved systems administration.

Vision and Scope for the Windows 2000 Enterprise Forest
Windows 2000 Steering Committee, March, 9 2001

MEMBERSHIP AND BENEFITS

Membership in the Windows 2000 Enterprise Forest is not mandatory. Agencies are invited to join through a process outlined in this Welcome Kit and are encouraged to discover the benefits that other agencies are discovering. These benefits are the goal and mission of this project and a win/win for all stakeholders. Your agency, your agency's managers, the State of Washington and taxpayers, all reap benefits from joining the Windows 2000 Enterprise Forest.

Goal Benefits	
Agency	• Realize economies of scale and shared knowledge • IT administration and application development is streamlined • Extensive system policy management improves system security and stability • Multi-agency project leverages shared environments, testing, management, governance and oversight • Enables inter-agency application sharing
Agency managers	• Realize more value for the dollar • Strategic piece of the Enterprise (Universal Framework) architecture • Improved intra-agency operations • Enabling architecture / system for business processes, security, communication, resource sharing and inter-agency functionality
State of Washington	• A fundamental element in Washington State's vision and leadership in statewide information sharing • Forward-looking foundational architecture • Business process enabler • Streamlined IT infrastructure • Improved collaboration and cooperation among agencies • Robust governance model (Comprised of multi-agency stakeholders)
Taxpayers	• Project focused on business results • Good stewardship of tax dollars through economies of scale and shared knowledge resources • Provides an architecture that will enable efficiencies within and between agencies that will benefit their customers and the citizen

While joining is voluntary, intra-agency collaboration and costs improve as more agencies are involved. We'd like to invite you to become part of this exciting step into the future! A description of how to join follows.

HOW TO JOIN THE WINDOWS 2000 ENTERPRISE FOREST

Joining the single-root forest requires the following steps[1]:

1. Development of your agency's Migration Plan to the Windows 2000 Enterprise Forest
2. Approval of your Migration Plan, with an accompanying signed DIS Service Level Agreement (See Appendix B.)
3. Implementation in the Pre-Production Forest based on your Enterprise Forest Migration Plan
4. A 30-day trial run in the Pre-Production Forest
5. Full production of the Enterprise Forest Migration Plan, with success of the test.

Before initiating a request to join the Enterprise Forest, your agency should read the following documents previously listed in the document tree:

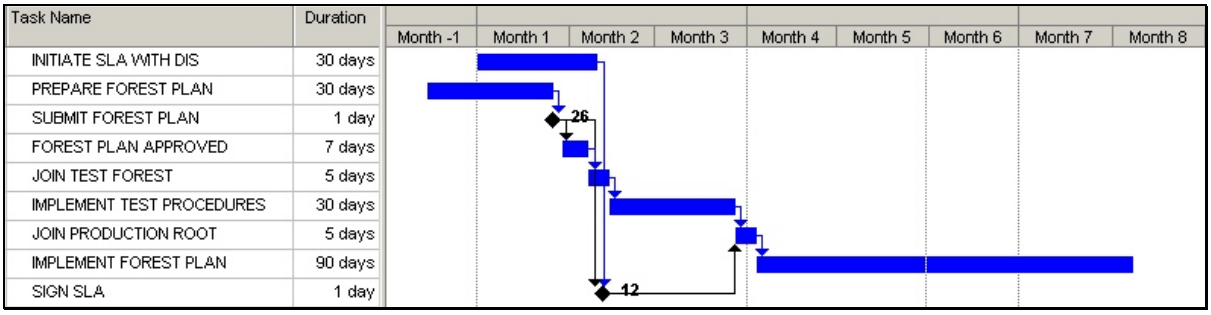
1. **Root Domain Requirements** (*Document* 2)**:** Identifies the structure, implementation of the root, and procedures for joining

2. **Naming Conventions and Standards Document** (*Document* 3)**:** Describes naming conventions and standards that all machines in the Forest must follow

3. **Agency Joining Procedures Document** (*Document* 5)**:** Describes the steps that agencies and root administrators must follow in order for the agency to join

4. **Change Management Document** (*Document* 6)**:** Describes the process for submitting change requests to the root. Changes might include site link connections, new agency joins, and schema changes.

Typically, the process for joining the single-root Forest will take an agency several months to complete. Figure 3 provides a timeline that agencies can use in their planning. Expect to spend an estimated 30 days preparing your agency's Windows 2000 Migration Plan. The Forest Resource Group, the technical authority and guidance team for the root, will review and recommend approval of your agency's Windows 2000 Enterprise Forest Migration Plan to the steering committee.



[1] A detailed diagram of the entire process can be found in Appendix A.

Figure 3 - Forest Root Join Timeline

Once your Migration Plan to the Windows 2000 Enterprise Forest is ready for review, you may request a Service Level Agreement (SLA) from the Department of Information Services (DIS). Terms of the SLA are subject to negotiation between the agency and DIS.

Once your Migration Plan is approved, you can begin implementing in the Pre-Production Forest. During this period, a series of quality assurance tests must be performed. This process usually lasts an estimated 30 days.

Note: If only minor changes are suggested for your Migration Plan, you can begin implementation in the Pre-Production Forest before final approval is received.

With success in the Pre-Production Forest and with a signed SLA, you are ready to move into production. The initial server join will be coordinated with DIS. Migration of subsequent servers, workstations, and users will be the responsibility of the agency.

The two sections that follow outline requirements for an agency's Windows 2000 Enterprise Forest Migration Plan and provide a list of specific tasks that must be completed.

PROCEDURES TO BE RUN IN THE TEST FOREST (REQUIRED)

To ensure that your test implementation is as close as possible to a production environment, you should design tests that perform tasks you ordinarily do. In order to ensure overall domain health before moving to production, there are some additional recommended tests that should be included, as well. A description of these tests follows.

Basic Tasks

The following basic tasks should be performed during the 30-day test period. Errors should be documented, escalated (if necessary) and communicated to DIS.

- Add a minimum of 5 workstations and users into your agency domain
- Verify that replication with the root hub is working and investigate any issues
- Verify that replication within the agency works, and that latency is no more than 15 minutes for new objects (such as users or computers)
- Perform a processor and memory utilization benchmark over a period of at least 5 days to ensure adequate hardware resources will be available in production
- Backup your Active Directory server and successfully restore it to an alternate machine.

Run Quality Assurance Scripts

There are four scripts that make up the quality assurance test. Each of these is described below, along with their interaction with each other.

The scripts are available in the Windows 2000 Resource Kit. Contact DIS Help Desk if you need copies of the scripts or assistance finding them.

QA_Check.cmd

This is the main script of the quality assurance test process. It records the current state of a domain controller when it is run. This script uses a variety of Microsoft Windows 2000 Resource Kit utilities and other scripts to obtain information about the domain controller, Active Directory replication, and FRS replication.

QA_Parse.vbs

This script is called by the **QA_Check.cmd** script and parses the data files created by the utilities and scripts run as part of the quality assurance test process. The script parses the data files to locate errors and potential issues, which are then written to a summary file. This summary file is then copied by the **QA_Check.cmd** script to a central server so that you have a single location to examine the state of your domain controllers.

CheckServers.cmd

This script is used on the central server that has the summary files from each domain controller and provides a status report on the health of the domain controllers in your environment. This script outputs a file that contains three lists of domain controllers:

1. Domain controllers that are healthy and did not report any errors
2. Domain controllers that reported errors and require further investigation
3. Domain controllers that did not report and should be investigated

CheckServers.vbs

This script is used by CheckServer.cmd to perform parsing of the summary files from your domain controllers and to determine into which list a domain controller should be placed.

Process for Using the Quality Assurance Scripts

Manually execute the QA_Check.cmd script from the command line.	1. Schedule **QA_Check.cmd** to run on every domain controller in your environment. This should be scheduled to run at least twice per week during the test phase. 2. Schedule **CheckServers.cmd** to run on the central server. This script should be scheduled to after all of the domain controllers have run the **QA_Check.cmd** file. 3. Use Notepad to examine the contents of the **C:\QAShare\Serverreport.txt** file to determine if any domain controllers have reported errors or did not report in the last quality assurance cycle. 4. If a domain controller reported errors, or did not report, you will need to investigate and resolve any errors. To start investigating errors, open the summary file under the **C:\QAShare\<*computername*>** folder. From there, you can then examine the detailed files on the domain controller itself. 5. If the summary file for a domain controller indicates that it reported errors, the above log files should be examined to determine the specifics of the error that was reported. The additional information in these log files will aid you in troubleshooting the error. In addition to examining the above files, you should also examine the event logs in Event Viewer to see if any events were logged that are related to the error.

Additional Information on QA Scripts

The **QA_Check.cmd** script uses utilities from the Microsoft Windows 2000 Resource Kit and several other scripts to record the state of a domain controller. **QA_Check.cmd** generates a large amount of data. This is why the script creates a summary file using **QA_Parse.vbs**. However, if a domain controller is reporting errors, you will need to examine the data files generated by the script. What follows are lists of the data files generated and the tools used to generate the files.

QA_Check.cmd creates the following files in the **C:\ADResults** folder on each domain controller on which it is run:

File	Contents
Dcdiag.txt	Output of running **Dcdiag.exe** to perform domain controller diagnostic checks.
Netdiag.txt	Output of running **Netdiag.exe** to check the network configuration and health of the domain controller. When running **Netdiag.exe**, the Lightweight Directory Access Protocol (LDAP) tests are skipped as they can place a large load on the network when there is a large number of domain controllers.
GPOstat.txt	Output of running **Gpostat.vbs** to verify that each Group Policy object is in sync.
Ntfrs_ds.txt	Output of running **Ntfrsutl.exe ds** to list the FRS view of the DS.
Ntfrs_sets.txt	Output of running **Ntfrsutl.exe** sets to list the active replica sets.
Ntfrs_inlog.txt	Output of running **Ntfrsutl.exe** inlog to enumerate the FRS inlog.
Ntfrs_outlog.txt	Output of running **Ntfrsutl.exe** outlog to enumerate the FRS outlog.
Ntfrs_version.txt	Output of running **Ntfrsutl.exe** version to list the application programming interface (API) and service versions.
Ntfrs_reg.txt	Output of running **Regdmp.exe** to output the contents of the **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NtFrs\Parameters** registry key.

Ntfrs_sysvol.txt	Output of running **Dir %*Systemroot*%\sysvol /s** to store a list of the contents of the SYSVOL folder.
Frsconstat.txt	Output of running **Connstat.cmd** to summarize the FRS connection state. For more details on what this script does, see "Monitoring FRS Replication with **Connstat.cmd**" later in this chapter.
Ntfrs_errscan.txt	Output of running Findstr to search the **%*windir*%\debug\ntfrs_*.log** files for "error", "invalid", "fail", "abort", and "warn".
Ntfrs_parse.txt	Output of running Findstr to search **%*windir*%\debug\ntfrs_0005.log** for "error", "invalid", "fail", "abort", and "warn".
Ntfrs_parse2.txt	Output of running **Findstr** to search **%windir%\debug\ntfrs_0005.log** for "ERROR - EXCEPTION (000006ba): WStatus: RPC_S_SERVER_UNAVAILABLE", "ERROR - STAGING AREA FULL", "ERROR - DISK_FULL", "ERROR_DISK_FULL", "ERROR - EXCEPTION EPT_S_NOT_REGISTERED", "has no inbound server", "has no outbound server", "DS: Multiple connections from", "WARNING: Setting FrsVsn - Current system Time has moved backwards from value in config record", and "JRNL_WRAP_ERROR".
Ds_showreps.txt	Output of running **Repadmin /showreps** to list the replication partners for the domain controller.
Ds_showconn.txt	Output of running **Repadmin /showconn** to list the connection objects for the domain controller.
Services.txt	Output of running Net Start to list the services that are running on the domain controller.

If the summary file for a domain controller indicates errors, the above log files should be examined to determine the specifics of the error. The additional information in these log files will aid you in troubleshooting. In addition to examining the above files, you should also examine the event logs in Event Viewer to see if any related events were logged.

What Does QA_Check.Cmd Do?

1. Copies any files in **C:\ADResults\<computername> to C:\ADResults\<computername>\old**. Doing so provides a history of the state of the domain controller.
2. Runs the Microsoft Windows 2000 Resource Kit utilities and other scripts. This generates a series of data files, one for each utility and script, and stores the data files in **C:\ADResults**.

   Note: Data files stored in **C:\ADResults** are over written each time **QA_Check.cmd** script runs.

3. Runs the **QA_Parse.vbs** script to generate a summary report for the domain controller. The summary report uses the domain controller's computer name and the current date and month for the file name, for example: **BO1DC-30-11.txt**. This file is stored in **C:\ADResults\<computername>**.
4. On the central server, copies the previous summary file to **\\<server>\QAShare\<computername>\old folder**.
5. Copies the new summary file to the central server specified in the **QA_Check.cmd** script. The file is copied to the **\\<server>\QAShare\<computername>** folder.

What Does CheckServers.Cmd Do?

1. Copies **C:\QAShare\Serverreport.txt** to **C:\QAShare\old**
2. Runs **CheckServers.vbs** to parse the summary files each domain controller copied to the central server, generating **C:\QAShare\Serverreport.txt**.

MIGRATION PLAN CHECKLIST (REQUIRED ITEMS)

1 Read the following required documents from the Windows 2000 Enterprise Forest Document Tree.

- ☐ Root Domain Requirements
- ☐ Naming Conventions and Standards
- ☐ Agency Joining Procedures
- ☐ Change Management Process

2 Submit your agency information, which should include:

- ☐ Agency name
- ☐ Agency domain administrator contact information, including at least two system administrators who can be on call 24 hours per day.
- ☐ The migration teams and personnel your agency has assigned to the Windows 2000 Enterprise Forest

3 Submit your agency technical information

- ☐ Agency domain name (Windows 2000)
- ☐ Name of first domain controller (production and test)
- ☐ IP address of first domain controller (production and test)
- ☐ At least one sub-net and site to be created. If you will have multiple sites, it is highly recommended your request include all sites
- ☐ Server hardware specifications for the production servers in your agency
- ☐ List of all Active Directory software applications, including those planned after your Windows 2000 Enterprise Forest deployment

4 Include a copy of your network documentation

- ☐ Logical diagram of agency links, sub-domains and sites. At a minimum, this can be a high level overview and need not include specific implementation details
- ☐ Domain Name System (DNS) zone diagram describing any agency-specific DNS requirements
- ☐ Site replication plan that includes the hours during which you intend replication to occur
- ☐ Clearly identified firewalls and proxies, especially those that hide Active Directory domain controllers from other agencies in the statewide network.

5 Include a migration plan.

- ☐ Domain upgrade path plan. Will you be doing an in-place upgrade, or migration?
- ☐ Strategy for upgrading domain controllers. Will you be using new servers, or existing ones?
- ☐ Project calendar, including dates you expect to be in test, production, etc., as well as specific requirements or demands relevant to your agency.

Next is a suggested list of additional items you may want to add to your Windows 2000 Enterprise Forest Migration Plan.

MIGRATION PLAN CHECKLIST (SUGGESTED ITEMS)

The following is a suggested list of items you might wish to add to your Windows 2000 Enterprise Forest Migration Plan. This is not all-inclusive. Your agency may want to add additional items.

- ☐ Define the Vision and Scope for your agency's project. This could include a description of your senior management's buy-off.
- ☐ List of all resource servers (domain controllers, file servers, web servers, mail servers, etc.).
- ☐ List of all applications maintained by your IT staff. As part of this list, indicate the extent to which each application has been tested, as well as any known issues with Windows 2000 or the Active Directory.
- ☐ Necessary schema changes. If you have applications that will require modification of the Active Directory schema, document these in your Migration Plan.
- ☐ Site design. This is a physical diagram of your site that defines geographic boundaries and wide area network links within your agency.
- ☐ Domain plan. This is a logical design for security and administrative delegation.
- ☐ Administration and security plans. How will security be implemented, audited, etc.?
- ☐ Post-upgrade tasks. What needs to happen after your migration, in order to resume normal operations?
- ☐ Procedures for maintaining network services during an upgrade. How will you minimize downtime and the impact on your customers?
- ☐ Group policy and system policies. What policies are in place, need to be modified?
- ☐ Plan for maintaining security during an upgrade. How will you ensure security?
- ☐ Plan for leveraging existing directory information. Will you be migrating from Exchange 5.5, or Novell NDS?
- ☐ Plan for related replication traffic. This impacts your site design.
- ☐ Plan for authentication traffic. This impacts your site design.
- ☐ Plan for cloning security principals, users and global and universal groups. This will be necessary in most cases where a migration is chosen over an in-place upgrade.
- ☐ List of migrating computers and local group accounts
- ☐ Plan for cloning local groups on domain controllers. How will you implement this feature?
- ☐ Plan for moving domain controllers. How do you plan to accomplish this?

Next we'll look at best practices for successfully completing your Windows 2000 Enterprise Forest Migration Plan.

BEST PRACTICES FOR YOUR ENTERPRISE FOREST MIGRATION PLAN

This section focuses on best practices to follow when planning your Windows 2000 Enterprise Forest migration.

Guiding Principles

The following principles should guide planning and designing of your agency's migration.

1. **Simplicity is the best investment**. Simple designs are easy to explain and maintain.
2. **Aim for the ideal design**. Review the components and decide where you want to go.
3. **Explore design alternatives**. The merit of a design emerges in comparison to others.
4. **Anticipate change**. How will change or reorganization affect your design? Plan knowing change will happen.

Simplicity Is the Best Investment

Simple structures are easier to explain, maintain, and debug. Although some complexity may add value, be sure to weigh the added value against potential maintenance costs in the future.

For example, optimization of query and replication traffic might require a complex site topology. However, such a topology is harder to maintain. Always analyze the tradeoffs before deciding on a complex structure. Justify the existence of any structure you create.

Aim for the Ideal Design

In your initial design, consider the ideal structure, even if it does not reflect the current domain or directory infrastructure, and even if the ideal design is not currently attainable. Weigh migration costs against the long-term savings of the ideal plan. Refine your design appropriately.

Explore Design Alternatives

Make more than one pass at each design. The value of a design becomes more evident when you compare it to other design ideas. Combine the best of all designs into the plan you implement.

Anticipate Change

Change occurs regularly within any organization and can range from employee moves to enterprise-wide reorganization. Change can affect your active directory structure. When designing the structure, consider how potential changes will affect user and administrator interaction with the directory. Make sure your design is general and flexible enough to accommodate constant and significant change. However, while anticipating change is an important aspect of design, it should not dominate the design process.

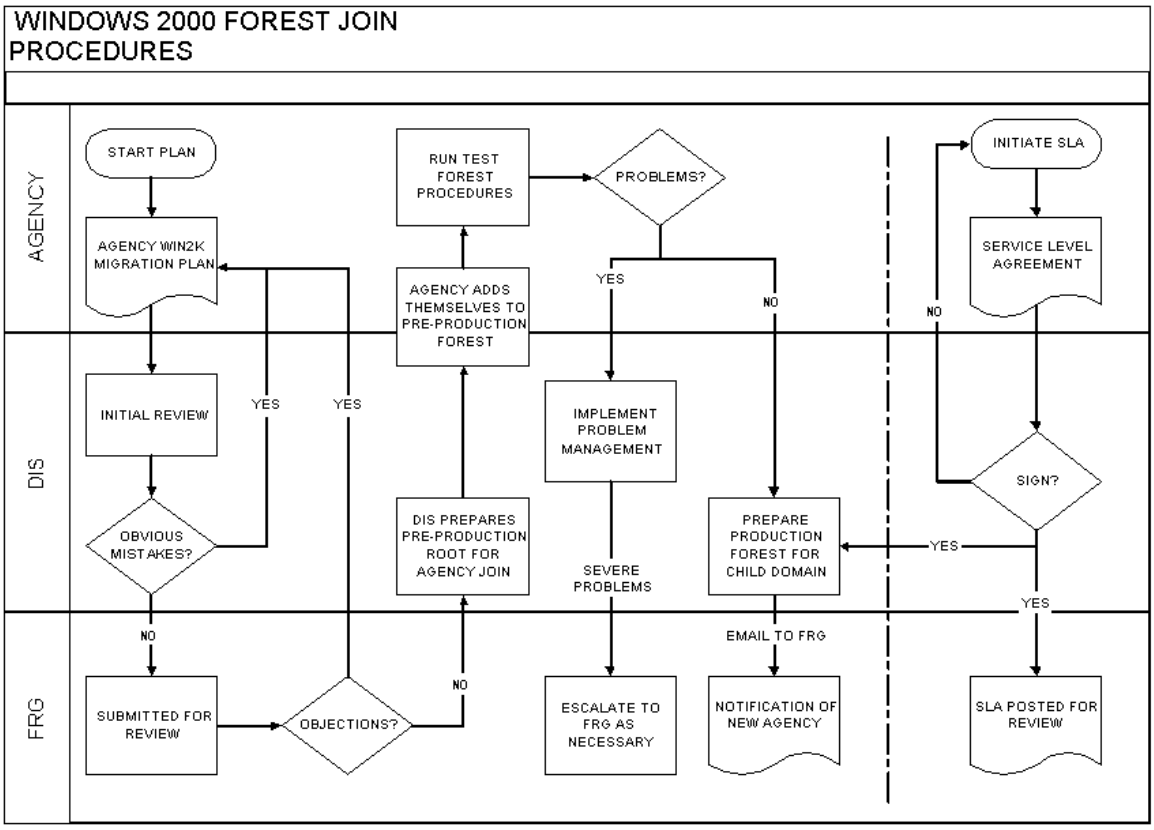
This completes our management overview of the Windows 2000 Enterprise Forest. More detailed technical information is included in Appendices to this document.

Appendices
FAQ's

As you begin your Windows 2000 Enterprise Forest Migration planning, your technical support people will have some questions. This section of the Welcome Kit provides answers to frequently asked technical questions (FAQs). For more in-depth information, refer your employees to the document tree for direction to the specific source of additional technical information.

APPENDIX A: Windows 2000 Enterprise Forest Join Process

A detailed process flow diagram of the Windows 2000 Enterprise Forest Join Process follows:



Forest Root Join Process Overview

The process can be summarized by the following five steps:

1. Development of your agency's 2000 Migration Plan to the Enterprise Forest
2. Approval of your Windows 2000 Migration Plan, with a signed DIS Service Level Agreement
3. Implementation in the Pre-Production Forest based on your Enterprise Forest Migration Plan
4. A 30-day trial run in the Pre-Production Forest
5. Full production of the Migration Plan with success in the Pre-Production Forest

APPENDIX B: Service Level Agreement

DIS Statewide Root Management Responsibilities

- Implement Windows 2000 Steering Committee policies
- Provide hardware and software for the Root Domains
- Maintain 99.9% availability of the Root Domain in the production environment
- Provide the Production, Pre-Production and Rip and Tear Forests
- Follow change control processes
- Administer the Root Domain
- Provide problem management
- Contract technical support from vendors
- Provide security administration
    - Protect customers from unauthorized use
    - Secure physical access
    - Implement Steering Committee security policy

Agency Responsibilities

- Maintain the agency's SLA
- Provide hardware and software for the agency Child Domain
- Designate technical support staff within the agency
- Participate in the Pre-Production Forest
- Follow security policies and procedures
- Follow change control policies and procedures
- Adhere to naming conventions and standards (Appendix E)

APPENDIX C: Applications under consideration

Department of Personnel Vision

The Department of Personnel is planning a full-featured human resources data service through the Windows 2000 Enterprise Forest. This will include employee IDs, a common employee database, training history, leave balance, and other personnel data from DOP.

Logon Assist Module (Single Sign-On) Prototype

In the current environment, users must remember too many passwords, developers spend too much time managing authentication and access control, help desks spend too much time resetting passwords, and managers can't set enterprise-wide access policies. With the Windows 2000 Enterprise Forest, users will need only one ID and password to access any computer application.

The Logon Assist Module authenticates the user to legacy applications without another logon ID. Each agency owning a legacy application on the Enterprise Forest can have their own version. Users are allowed access to an application if the user's group matches the permission list. For highly secure applications, owners may require re-authentication.

The following agencies are prototyping the Logon Assist Module: L&I, GA, DSHS, DOP, DIS, OFM and ESD. This prototype activity will validate implementing this application across the Enterprise Forest.

APPENDIX D: The DFC Process

As the Enterprise Forest implementation proceeds, participating agencies are making discoveries and developing best practices that can be valuable to others. To share this information, the Draft for Comment (DFC) process has been established. This permits any one to quickly draft DFC's, which are stored in a repository for others to reference. Any agency joining the Forest should search the DFC repository for planning and operating ideas.

The content of a technical draft may be any thought, suggestion, etc., related to the Enterprise Forest. Suggestions are not limited to specific product lines or vendors. Initial drafts are to be timely rather than polished. A DFC should include, at a minimum, the following three paragraphs: 1) purpose, 2) "applies to," and 3) summary (which can include details).

To ensure consistency of technical documentation in the Forest, the Forest Resource Group has adopted the following standards for authors to follow when proposing new standards or best practices. These standards apply to all authors of technical documentation drafts in the Enterprise Forest.

Standard

1. Documentation must be written in Microsoft Word and saved in a .doc format.
2. Documentation may include text, images, diagrams, spreadsheets, etc., but all external content must be embedded (no linked content).
3. All documents must have a Draft ID (serial number), provided by the Forest Root Administrators.
4. All pages in the draft should contain a header with the title, status, draft ID, what that draft supercedes, status and author. (A template is available that automatically provides this format.)
5. The document must contain three sections: purpose (business case), applies to (who should read), and summary (what should they do). Additional sections are optional at the author's discretion.

Document Status Levels

A technical draft will have one of three status levels:

1. **Draft for Comment** status level means the DFC is unpolished or incomplete. This level encourages immediate distribution of drafts so feedback from other agency members can be collected as quickly as possible.
2. **Recommended** status level means the Forest Resource Group has decided the DFC should be implemented as a best practice in the Forest. This means Administrators should regard Recommendations as requirements, unless business objectives prohibit compliance.
3. **Required status** level means the DFC should be implemented as a matter of policy on all applicable Forest-wide resources. To achieve the "Required" status, a DFC must be approved at the Forest Resource Group and Steering Committee levels.

APPENDIX E: Training

A fundamental element of any major operating system implementation or migration is an initial assessment of the technical staff's knowledge base. Well-planned and structured training may be essential to provide the staff with the skills needed to design, implement and support the system. Lessons learned and best practices indicate that skills and knowledge levels be commensurate with the scope and requirements of the project.

The Microsoft Official Curriculum (MOC) classes and the training track outlines are intended as a guide to assist project managers, staff and managers in determining their training requirements. Complete descriptions of the class content can be obtained from any official Microsoft Training provider.

SKILLS FOR MICROSOFT TECHNOLOGY PROFESSIONALS

Windows 2000 Deployment Framework

We've listed the recommended training classes by role.

Role: ARCHITECT/DESIGNER

planning and design phase	1560 Upgrading Support Skills from NT 4 to Win2k
	1561 Designing a Directory Services Infrastructure
	1562 Designing a Networking Services Infrastructure
	2010 Designing a Win2k Migration Strategy
	2150 Designing a Secure Win2k-based Network

Role: NETWORK ENGINEER

design and deployment phase	2152 Supporting Win2k Professional and Server
	Engineer with INFRASTRUCTURE FOCUS: 2153 Supporting a Networking Infrastructure
	Engineer with ACTIVE DIRECTORY FOCUS: 2154 Implement/Administer Win2k Directory Services
	2150 Designing a Secure Win2k-based Network
	2010 Designing a Win2k Migration Strategy
	1561 Designing a Directory Services Infrastructure

Role: NETWORK ADMINISTRATOR

deployment phase	2152 Supporting Win2k Professional and Server
	2153 Supporting a Network infrastructure
	2154 Implement/Administer Win2k Directory Services
	1561 Designing a Directory Services Infrastructure

Role: HELP DESK

support phase	A+ Certification
	2151 Win2k Network and Operating System Essentials
	2152 Supporting Win2k Professional and Server

Skills for Microsoft Technology Professionals

Developer Readiness Framework

ROLE: OBJECT-ORIENTED DEVELOPER

move from mainframe applications to object-oriented applications

- 1587 Introduction to Programming
- sd201 Access Programming
- 1303 Mastering Visual Basic 6 Fundamentals
- 1633 Building Data Centric- Business Applications
- 2071 Querying SQL Server 2000 with Transact-SQL
- 1013 Mastering Visual Basic 6.0 Development

Role: ADVANCED DEVELOPER

for the Visual Basic developer moving to enterprise applications

- 1013 Mastering Visual Basic 6.0 Development
- 2071 Querying SQL Server 2000 with Transact-SQL
- 2073 Implementing a Database Design on SQL Server 2000
- Sd298 Combines 1587 Gathering and Analyzing Business Requirements and 1609 Designing Data Services and Models
- 1608 Designing Business Solutions
- 1016 Designing and Implementing Distributed Applications

Role: WEB DEVELOPER

for new-to-web developers

- 1912 Introduction to Web Development Technologies
- 1080 Essentials of VB Scripting for Web Site Development
- 1017 Mastering Web App Development using Visual InterDev
- 1905 Building XML-Based Web Applications
- 1913 Exchanging and Transforming Data using XML and XSLT
- 2379 Developing and Deploying Biztalk Server 2000 Solutions